

Maturing A Security Program to Support the New Texas Higher Education Strategic Plan



Texas Higher Education
Coordinating Board

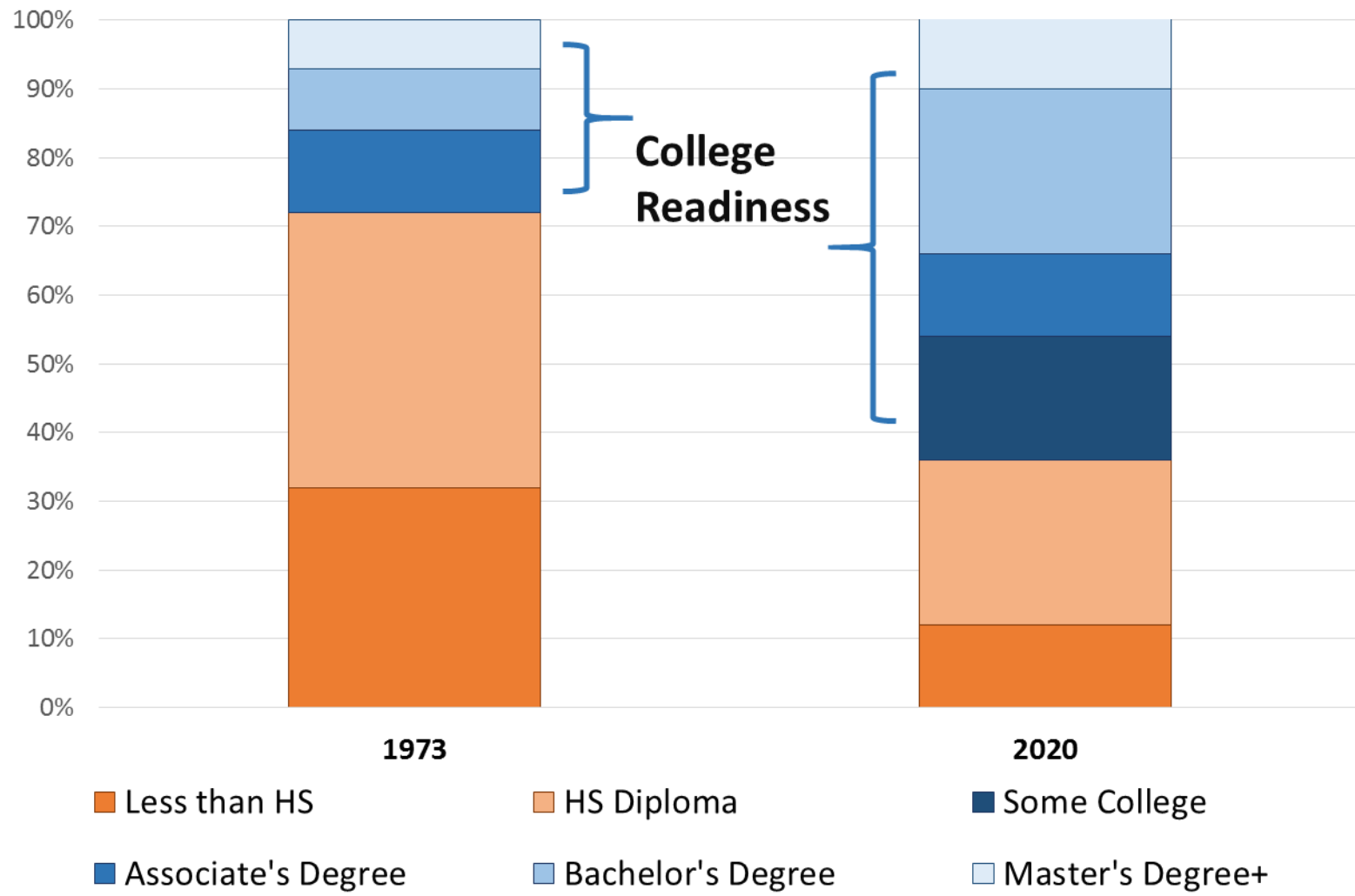
John House, CISSP
Information Security Officer
Texas Higher Education Coordinating Board

Agenda

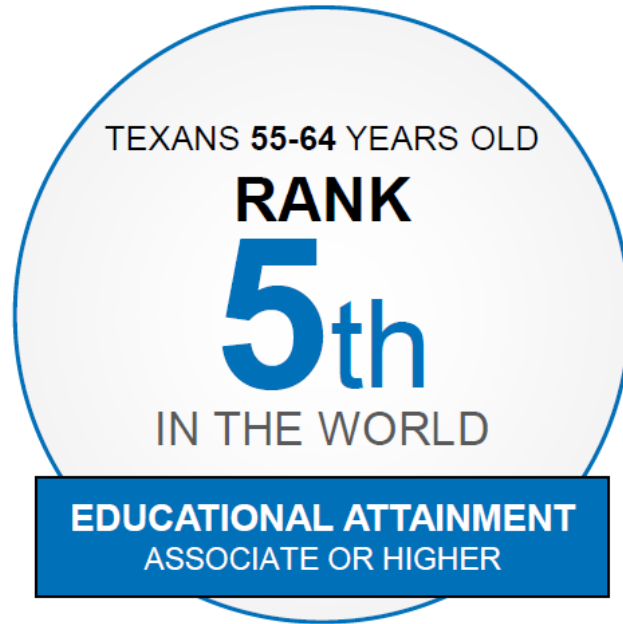
- 60x30TX
- Maturity Measures
- Information Security Assessments
- Risk Assessment
- Engagement

**Higher education is
more important
than ever.**

More U.S. Jobs Will Require Postsecondary Educationand thus more College Ready Students



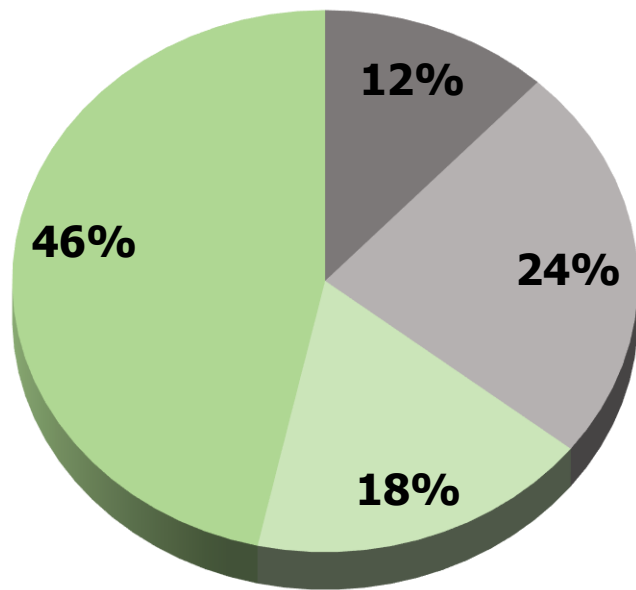
TEXAS IS LOSING GROUND



Texas attainment levels have stayed relatively steady,
but in a global economy, **staying steady = falling behind**

According to the Center on Education and the Workforce, our future workforce **will demand more** postsecondary trained and educated workers.

U.S. Workforce Projections by
Required Education Level, 2020



■ H.S. Dropout

■ H.S. Grad

■ Some college, including Certificates

■ Associate's degree or higher

In 1973, only 28% of all U.S. jobs required postsecondary education/skills. By 2020, **59% of the jobs** in Texas will require this level of education.

Currently, **38%** of Texans have an certificate or degree

Source: Georgetown University, Center on Education and the Workforce; data in charts rounded.

Jobs Gained Nationally During the Financial Recovery of 2010-2016



80K

Completing high school or less



3.1M

With an associates degree or
some college



8.4M

With a bachelor's degree or
higher

60x30TX – What can we do to raise the bar?

Four Student-Centered Goals



THE OVERARCHING GOAL: 60x30

At least 60 percent of Texans ages 25-34 will have a certificate or degree.

☒ *Supports the economic future of the state*



THE SECOND GOAL: COMPLETION

At least 550,000 students in 2030 will complete a certificate, associate, bachelor's, or master's from an institution of higher education in Texas.

☒ *Requires large increases among targeted groups*



THE THIRD GOAL: MARKETABLE SKILLS

All graduates from Texas public institutions of higher education will have completed programs with identified marketable skills.

☒ *Emphasizes the value of higher education in the workforce*



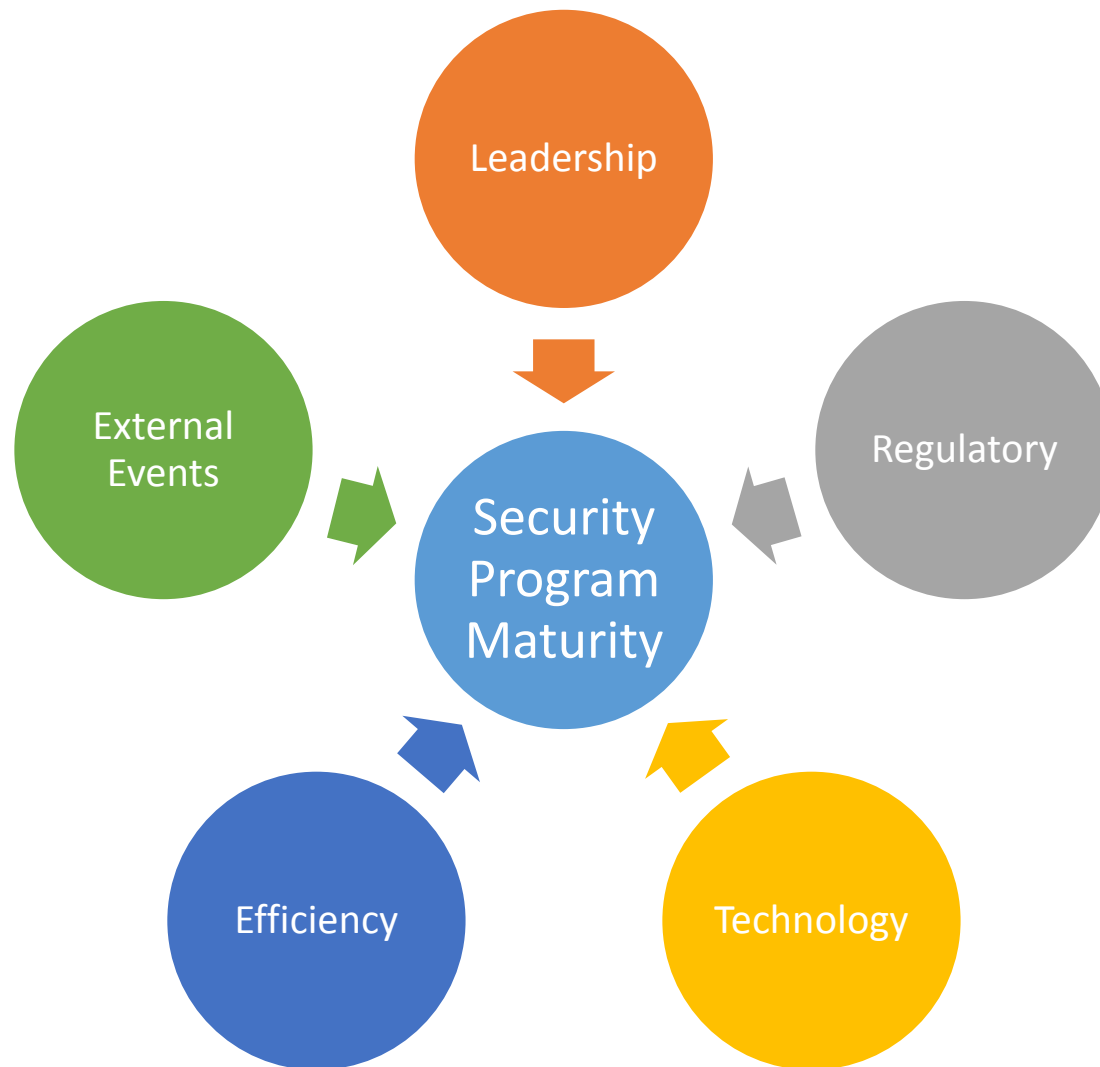
THE FOURTH GOAL: STUDENT DEBT

Undergraduate student loan debt will not exceed 60 percent of first-year wages for graduates of Texas public institutions.

☒ *Helps students graduate with manageable debt*

**Information Security
is more important
than ever.**

Security Program Stimulators



Maturity Measures – Self Assessment

The self-assessment starting point.


Regulatory – Texas Cybersecurity Framework

- 40 Objectives

Self-assessment

- Security Control Standards Catalog
- SPECTRIM - Agency Security Plan
- SPECTRIM - Risk Management
 - Organization / Networks / Applications /Facilities
- Other

Maturity Level	Description
0	None, no evidence
1	Ad-hoc, reactive
2	Consistent, mostly reactive
3	Documented, detailed
4	Risk based, managed
5	Efficient, Optimized

 NIST-R0003-AC-03.02: Are information systems (Application Assessments; operating systems; Network Assessment devices; databases; etc.) configured and access enforcement mechanisms employed per approved policy to provide protection from unauthorized access by malicious users; software or systems?

- ☒ Implemented
- ☐ Partially Implemented
- ☐ Not Implemented
- ☐ Unknown
- ☐ Not Applicable

Maturity Measures

Third Party Assessments

Embrace third party assessments.

- THECBs use of DIR Funded Security Assessments
- Success with organizational change
 - Gartner Information Security Assessment (THECB 2013)
 - Vendor presents to the Board
 - Regular updates from IRM and ISO to the Agency Operating Committee
 - Success with appropriation request
 - NTTData (THECB 2017)
 - Regular security updates to the IT Steering Committee
 - Continued status updates to the AOC

Assessment Results

- **Expect reports**
 - **Baseline Report**
 - **Assessment Report - Findings & Recommendations**
- **Pay attention to drafts**
- **Expect recommendations**
 - **Maturity 2 – 16**
 - **Maturity 3 - 24**
- **Specific mandates to mature the security program**
- **Implementation Roadmap**
- **Findings can be general - Be creative with action plans**

Risk Assessment Priority

Use Risk Assessment to direct efforts to mature the security program

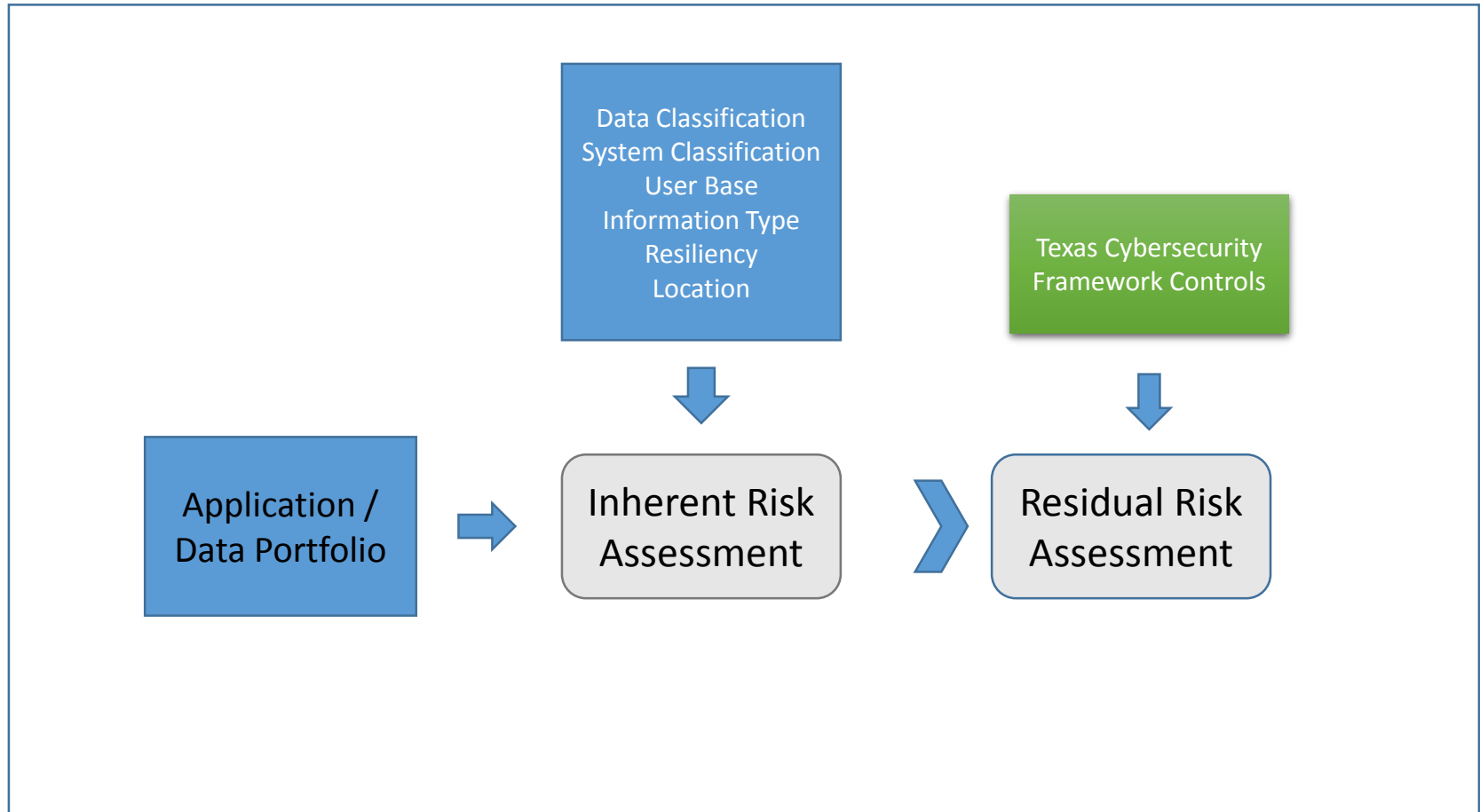
- Risk Assessment central to resolution of assessment roadmap
 - Information Security Risk Management
 - Critical Information Asset Inventory
 - Secure Configuration Hardening & Patch Management
 - Security Awareness and Training
 - Systems Communication Protection
 - Cloud Usage and Security
- **Asset Inventory needs**
 - Asset inventory updates and accuracy for data and portfolio management
 - Designate mission critical applications
- **Drive awareness of portfolio and responsibilities**
 - Engage Owners and educate regarding data ownership responsibilities

What can we do?

Risk Assessment Approach

- Requirements for a practical risk assessment tool
 - Estimates “Inherent” and “Residual” risk
 - Provides update for Information Resources Deployment Review and SPECTRIM Risk Assessment
 - Consideration of standard controls
- Classification Based Risk Assessment Method (CBRAM)
- Two-step model:
 - Assess Inherent Risk based on 6 weighted criteria
 - Assess Residual Risk based on controls assessment

CBRAM Risk Assessment Model



Drive knowledge of Inherent Risk

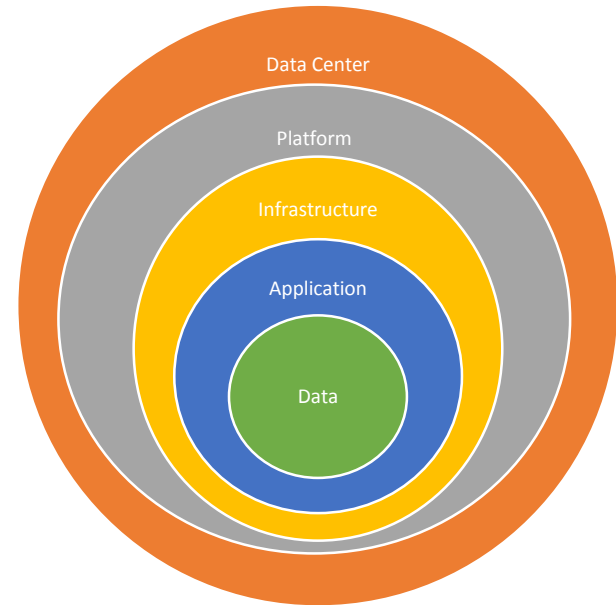
- TAC 202 risk terminology

Inherent Risk

- Inherent Risk is not based on what security controls are implemented within an application/system, but it is more about what it does for the business, what goes around it, data, system and users.

Residual Risk

- Based on what controls are in place and how effective the controls are to prevent threats/vulnerabilities
- Estimated based on presence of Controls



Inherent Risk Assessment Model

Factors and Weighting

Six criteria are considered in the inherent risk assessment. The weight of criteria can be adjusted based on changes in environment, priorities, strategy or risk tolerance.

	Definition	Weight
Data Classification	Looks at the sensitivity of the data based on risks to confidentiality and integrity of the data.	30%
Systems Classification	Sensitivity of the system – Mission Critical or other	30%
User Base	People who use the system	10%
Information Type	Information Type processed by the application	10%
Resilient Infrastructure	Does the application have centrally managed disaster recovery processes	10%
Deployment Location	Location of the core infrastructure of the application	10%

1 - Data Classification

- High risk
 - Confidential Data
- Low Risk
 - Public Data Classification

Criteria #1

Data Classification

- 5 – FERPA Confidential
- 4 – Confidential
- 3 – Sensitive
- 2 – Public

Weight

30%

2- Criticality

Business Criticality

- **Mission Critical** – Immediate loss of revenue
- **Business Critical** – Some revenue loss
- **Business Operational** – sustained outage causes function loss
- **Business Administrative** – sustained outage and no loss

Criteria #2

Criticality

- 5 – Mission Critical
- 4 – Business Critical
- 3 – Business Operational
- 2 – Business Administrative

Weight

30%

3 - User Base

- High risk
 - Individual accounts and credentials
- Low Risk
 - For general use

Criteria #3

User Base

- 5 – Individual/Student
- 4 – Institution
- 3 – Agency/Vendor
- 2 – Authorized Staff
- 1 – General Internal Use

Weight

10%

4 - Information Type

- Basis - NIST 800-60 *Guide for Mapping Types of Information and Information Systems to Security Categories*
- Needed for feeding portfolio SPECTRIM in the future

Criteria #4

Information Type

Weight

10%

- 5 – Personal Identity & Authentication
- 5 – Security Management
- 4 – Funds Control
- 4 – Accounting
- 3 – Higher Education
- 3 – Goods Acquisition
- 2 – Information Sharing

5 – Resilient Infrastructure

Infrastructure

Based on disaster recovery testing

Undefined – no recovery server

Partial test – some DR testing

Full test – DCS recovery tested

Diverse – Cloud based on fully replicated

Criteria #5

Resilient Infrastructure

Weight

10%

- 5 – Undefined
- 4 – Designated recovery server
- 3 – Partial test
- 2 – Full test
- 1 – Diverse / Replicated

6 Deployment Location

More risk – Hybrid Cloud

Less Risk – Private Data Center

Weight

10%

Criteria #6

Deployment Location

5 – Hybrid Cloud

4 – Community Cloud

3 – Public Cloud

2 – Private Cloud

1 – Private Data Center

Spreadsheet Based Collection

Name	Description	Application Owner	C1 Data Classification 30%	C2 System Classif. 30%	C3 User Base 10%	C4 Information Type 10%	C5 Resiliency 10%	Deployment Location 10%	Data Classification Score	Systems Classification	User Base	Criticality of Dependant Business	Resilient Infrastructure	Deployment Location	Inherent Risk
Example Application Name 10	This is an example description for demo	DIVISION3/DEPT4	FERPA-Confidential	C3 Business Operational	Authorized Staff	Accounting	Defined	Private Data Center	5	3	2	4	4	1	3.5
Example Application Name 11	This is an example description for demo	DIVISION3/DEPT4	FERPA-Confidential	C3 Business Operational	Authorized Staff	Accounting	Defined	Private Data Center	5	3	2	4	4	1	3.5
Example Application Name 17	This is an example description for demo	DIVISION3/DEPT4	Confidential	C4 Business Administrative	Public/Student	User Fee Collection	Defined	Private Data Center	4	2	5	4	4	1	3.2
Example Application Name 3	This is an example description for demo	DIVISION3/DEPT4	FERPA-Confidential	C1 Mission Critical	Authorized Staff	Accounting	Defined	Private Data Center	5	5	2	4	4	1	4.1

Inherent Risk Assessment – Risk Level by Score

- Scored as a weighted average of the six criteria

$$= ((O55 * 0.3) + (P55 * 0.3) + (Q55 * 0.1) + (R55 * 0.1) + (S55 * 0.1) + (T55 * 0.1))$$

- Applications over 4.0 (Critical & High) would get a Residual Risk Assessment

Criteria Value	Inherent Risk Score
Critical	≥ 4.5
High	4.4 – 4.0
Medium	3.9 – 3.0
Low	2.0 and below

CBRAM - Residual Risk Score

- Evaluation of controls
 - **Goal – to be similar to the SPECTRIM residual score**
 - DIR Security Controls Standards Catalog version 1.3
 - SPECTRIM Risk Assessment has questions about the controls to score residual risk
 - Excel used to score estimate control compliance
- The formula –
 - Each control –
 - 2 = Implemented
 - 1 = Partial
 - 0 = Not/Applicable
 - -2 = Not Implemented
 - The controls are factored together into a percentage score

- Control compliance score
 - 1 to 5 based on percentage
 - 5 would be high risk or $< 85\%$
 - 1 would be low risk or $> 95\%$
- Residual Risk score is the Inherent risk reduced depending
- We will capture a baseline Residual risk score and as controls are implemented we can show a change in residual risk scores

[illegible]

Risk Assessment - Engagement

- Keep meetings to a minimum
- Owner updates
 - data classifications
 - What's mission critical?
- Use the session as a role-based training exercise
- Show owners processes that enable security governance
- Executive Participation

Assessment Lessons Learned

Security Assessment

- Do your homework
 - Get your Agency team on board
 - Brief any invited staff members
- Schedule Wisely
 - Find a spot where key staff will be available
 - ISO and IRM are in most meetings
- Close the loop
 - Board Presentation / Funding Request
 - Track progress on Roadmaps & Action Plans

THECB Control Objective Maturity Scores

Maturity Level	Number of Objectives
Level 3	??
Level 2	??
Total	40



Thanks!

John House

Texas Higher Education Coordinating Board
Information Security Officer

John.House@theccb.state.tx.us

Visit the 60x30TX website -

<http://www.60x30TX.com>